TITLE:

Information dynamics of cellular automata : CA computation and information theory (New Aspects of Theoretical Computer Science)

AUTHOR(S):

Nishio, Hidenosuke; Saito, Takashi

CITATION:

Nishio, Hidenosuke ...[et al]. Information dynamics of cellular automata : CA computation and information theory (New Aspects of Theoretical Computer Science). 数理解析研究所講究録 2003, 1325: 197-202

ISSUE DATE:

2003-05

URL:

http://hdl.handle.net/2433/43197

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録 1325 巻 2003 年 197-202

Information dynamics of cellular automata: CA computation and information theory*

Hidenosuke Nishio (西尾英之助　元・京大・理) †
Iwakura Miyake-cho 204, Sakyo-ku, Kyoto

Takashi Saito (斉藤隆　大工大・情報)
Faculty of Information Science, Osaka Institute of Technology

April 9, 2003

1 Introduction

Using polynomials over finite fields, we formulated the *polynomial state* cellular automata based on the *information variable* X for investigating informational phenomena arising from cellular dynamics[Nishio&Saito03]. In our youngest paper, we endowed X with the probability distribution $\{p(x)\}$ and established the *information theory of CA* in Shannon's sense. We showed that the entropy of configurations generally decreases by the cellular computation[Nishio&Saito02]. Here we are going to extend the theory to n-information variables and also try to utilize Kolmogorov complexity as another measure of information amount contained by configurations. As for the information theory and its relation to Kolmogorov complexity we refer to [Cover&Thomas91].

2 Preliminaries

2.1 CA defined by polynomials over finite fields

One-dimensional CA is usually defined with the space Z (the set of integers), the neighborhood N, the state set Q and the local function f and denoted as CA=(Z,N,Q,f). Throughout this paper we assume the 1-D CA with $N = \{-1,0,+1\}$ and denote simply as CA=(Q,f).

State Set: Q is assumed to be a finite field GF(q), where $q = p^n$ with prime p and positive integer n. Denote the cardinality of Q as $|Q|$. So $|Q| = q = p^n$.

*extended abstract

†corresponding author. E-mail: YRA05762@nifty.ne.jp

Local Function: The local function $f : Q \times Q \times Q \to Q$ is uniquely expressed by the polynomial form:

$$f(x,y,z) = u_0 + u_1 x + u_2 y + \cdots + u_i x^h y^j z^k + \cdots + u_{q^3-2} x^{q-1} y^{q-1} z^{q-2} + u_{q^3-1} x^{q-1} y^{q-1} z^{q-1}, \quad \text{where } u_i \in Q \ (0 \le i \le q^3 - 1). \quad (2.1)$$

x, y and z assume the state values of the neighboring cells -1(left), 0(center) and $+1$(right), respectively.

Global Map: The set of configurations is $C = Q^Z$. The global map or the CA map $F : C \to C$ is defined as usual. Let $c(i)$ be the state of cell $i \in Z$ of configuration $c \in C$. The configuration at time t is denoted by c^t. $F^t(c^0) = c^t$. So, the state of cell i at time t is denoted by $c^t(i)$.

2.2 Information X and Extended CA$[X]$

Information X: Let X be a symbol different from those used in the polynomial form (2.1). It stands for an unknown state or the *information* of a cell in CA and will be called the *information variable*. In order to investigate the dynamics of information X in CA space, we consider another polynomial form, which generally defines the cell state of the *extended* CA.

$$g(X) = a_0 + a_1 X + \cdots + a_i X^i + \cdots + a_{q-1} X^{q-1}, \quad \text{where } a_i \in Q \ (0 \le i \le q - 1). \quad (2.2)$$

g uniquely defines a function $Q \to Q$ and the set of such functions is denoted by $Q[X]$. Evidently $|Q[X]|=q^q$.

Extended CA$[X]$ or Polynomial State CA: Based upon CA$=(Q, f)$ we define its *extension* CA$[X]=(Q[X], f_X)$, where the set of cell states is a polynomial ring $Q[X]$ as defined above. The local function f_X is defined on the same neighborhood and expressed by the same polynomial form f as was defined by (2.1). The variables x,y and z, however, move in $Q[X]$ instead of Q. CA$[X]$ will be called the *polynomial state* CA.

2.3 n-Information Variables

Consider n indeterminates (information variables) $X_1, X_2, ..., X_n$ to be introduced into the initial configuration: $c^0 = wX_1X_2...X_nw'$. As is in the preceding section the cell state $c^0(0)$ is considered to be X_1. Thus $c^0(i-1) = X_i$ for $1 \le i \le n$ and the other cells have constants. At time t effects of information variables $X_1, X_2, ..., X_n$ in c^0 possibly appear at cells $\{c(i) | -t \le i \le t + n - 1\}$ of configuration c^t. In order to discuss such a cellular development, we need to extend the basic CA to n-variable polynomial state CA.

Extension of CA to CA$[X_1, X_2, ..., X_n]$ is made similarly as CA$[X]$. The state set $Q[X_1, X_2, ..., X_n]$ constitutes of polynomials of the form;

$$g(X_1, X_2, ..., X_n) = a_0 + a_1X_1 + a_2X_2 + \cdots + a_hX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} + \cdots + a_{q^n-1}X_1^{q-1}X_2^{q-1}\cdots X_n^{q-1}, \quad \text{where } a_h \in Q \ (0 \le h \le q^n - 1). \quad (2.3)$$

The local function f is the same as Equation(2.1).

2.4 Substitution

Definition 1 Substitution: *For a polynomial $g \in Q[\mathbf{X^n}]$ and an n-tuple of symbols $\mathbf{a^n} = (a_1, a_2, ..., a_n)$, where $a_i \in Q$, we define the substitution $\psi_{\mathbf{a^n}}(g)$ as the state which is obtained by substituting a_i for X_i, $1 \le i \le n$. Substitution for a global configuration c $\{\psi_{\mathbf{a^n}}(c)|\mathbf{a^n} \in Q^n\}$ is defined, as in one variable case, by substituting the polynomial state of each cell with $\mathbf{a^n}$.*

Evidently we have, for any $c \in Q[\mathbf{X^n}]^Z$, $1 \le |\{\psi_{\mathbf{a^n}}(c)|\mathbf{a^n} \in Q^n\}| \le |Q|^n$.

We need the following commutative properties which are easily proved.

Proposition 2.1 *(1) Substitution $\psi_{\mathbf{a^n}}$ and ring operations of polynomials commute each other. That is, let g and h be polynomials in n indeterminates, then we have, for any $\mathbf{a^n} \in Q^n$,*

$$\psi_{\mathbf{a^n}}(g + h) = \psi_{\mathbf{a^n}}(g) + \psi_{\mathbf{a^n}}(h) \quad \text{and} \quad \psi_{\mathbf{a^n}}(g \cdot h) = \psi_{\mathbf{a^n}}(g) \cdot \psi_{\mathbf{a^n}}(h). \quad (2.4)$$

(2) The global map and the substitution commute each other.

$$\psi_{\mathbf{a^n}}(F_X(c)) = F(\psi_{\mathbf{a^n}}(c)), \forall \mathbf{a^n} \in Q^n. \quad (2.5)$$

2.5 Degeneracy

Definition 2 (Degeneracy) *In $CA[\mathbf{X^n}]$, a configuration c is called m-degenerate if $|\{\psi_{\mathbf{a^n}}(c) \mid \mathbf{a^n} \in Q^n\}| = |Q|^n - m$, where $0 \le m \le |Q|^n - 1$. Such m will be called the degree of degeneracy of c and denoted as $m(c)$. A configuration c is simply called degenerate if $m(c) \neq 0$.*

Theorem 2.2

$$m(c) \le m(F(c)) \quad (2.6)$$

3 Information Theory of CA Dynamics

For defining the quantitative measure of information amount transmitted or lost through the CA space-time development, we are going to exploit Shannon's information theory, in particular the mutual entropy and the channel capacity for the *deterministic* channel.

3.1 Deterministic Channel

We shortly recall Shannon's information theory, so that it may fit in with our formalism. Let X be a random variable of the information source, which takes a value $x \in Q$ with probability $\{p_X(x), x \in Q\}$. $p_X(x)$ will be abbreviated as $p(x)$. Shannon's entropy $H(X)$ is defined by,

$$H(X) = -\sum_{x \in Q} p(x) \log p(x) \tag{3.1}$$

Let us consider a *deterministic* communication channel (X, g, Y), where $g : Q \to Q$ is a function from Q to Q. That is a source symbol x in Q is sent by the sender and the receiver receives the symbol $y = g(x) \in Q$ with conditional probability $p(y|x) = 1$. $Y = g(X)$ is naturally a random variable and its probability distribution is calculated by the following formula.

$$p(y) = \sum_{x \in g^{-1}(y)} p(x). \tag{3.2}$$

The mutual information $I(X;Y)$ is defined by $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$.

Since the channel is deterministic we see that $p(y|x)$ is equal to 1 or 0. Therefore we have the followings; $H(Y|X) = 0$ and $I(X;Y) = H(Y)$.

The channel capacity is defined as follows:

$$C = \max_{p(X)} I(X;Y) = \max_{p(X)} H(Y) \tag{3.3}$$

3.2 Entropy of Configurations

Here we assume the information varibale X to be a *random variable* and are going to investigate *how much information* of the initial state is transmitted or lost during CA computation.

We interpret the correspondence between the CA dynamics and the communication theory as follows; the initial configuration containing an unknown state X at cell 0 corresponds to the information source, while the configuration c^t which contains $2t + 1$ polynomial states does the received message. We begin with one variable case. Let's take the portion of a configuration $c = (c(-t), c(-t+1), ..., c(0), ..., c(t-1), c(t))$, where $c(i)$ is the polynomial state (random variable) of cell i. The other cells contain constant states and can be ignored. The probability $p(c) = \{p(c_a)|a \in Q\}$ is calculated by the following equation.

$$p(c_a) = \sum_{x \in g^{-1}(c_a)} p(x), \tag{3.4}$$

where g is a function $X \to c$ such that $g(x) = (c(-t)(x), c(-t+1)(x), ..., c(0)(x), ..., c(t-1)(x), c(t)(x))$. The entropy of c^t is given by

$$H(c^t) = -\sum_{a \in Q} p(c_a^t) \log p(c_a^t). \tag{3.5}$$

Theorem 3.1

$$H(c^t) \geq H(c^{t+1}), \forall t \geq 0. \tag{3.6}$$

3.3 Channel Capacity

Though it is generally not easy to compute the channel capacity for arbitrary channels, we can present a formula for the deterministic ones. Let (X, Y) be a channel, where $Y = g(X), g : Q \to Q$. The channel capacity C is given by (3.3) and therefore our task is to compute max $H(Y)$ over $\{p(X)\}$. Using (3.2) we have,

$$H(Y) = -\sum_{y \in Q} \left(\sum_{x \in g^{-1}(y)} p(x) \right) \log \left(\sum_{x \in g^{-1}(y)} p(x) \right). \tag{3.7}$$

The entropy function H with n components generally takes the maximum value $\log n$, where the distribution is uniform. Note that the maximum is attained when each partition of Q defined by g^{-1} has the same probability and the distribution within a partition block is arbitrary.

$$p(g^{-1}(y)) = \frac{1}{|g(Q)|} \tag{3.8}$$

If $g^{-1}(y)$ is vacant, then $p(y) = 0$. Consequently we have,

Theorem 3.2

$$C = \max_{p(X)} H(Y) = \log |g(Q)|. \tag{3.9}$$

Theorem 3.3

$$C^t = \max_{p(X)} H(c^t) = \log \left(|Q| - m(c^t) \right) \tag{3.10}$$

Theorem 3.4

$$C^t \geq C^{t+1} \text{ for any } t \geq 0. \tag{3.11}$$

3.4 n-Information Variables

We generalize the idea of one variable case to n variable CAs. Let $\mathbf{X^n} = (X_1, X_2, ..., X_n)$ where X_is are identically distributed independent random variables with distribution $\{p(x)\}$. If the initial configuration is assumed to be $c^0 = wX_1X_2...X_nw' = w\mathbf{X^n}w'$, then its entropy is given by $H(c^0) = H(\mathbf{X^n}) = nH(X)$. For n-variable CA the similar monotone decreasing properties of $H(c^t)$ and C^t hold as one-variable CA. Particularly we have,

Theorem 3.5

$$C^t = \max_{p(X)} H(c^t) = \log \left(|Q|^n - m(c^t) \right) \tag{3.12}$$

4 Kolmogorov complexity of configurations

We are utilizing the following theorem about the conditioned Kolmogorov complexity and entropy. Let $\mathbf{X^n} = \{X_i, 1 \leq i \leq n\}$ be identically distributed independent random variables which take the value x in a finite alphabet Q with probability $p(x)$.

Theorem 4.1 (Kolmogorov) *Let* $p(\mathbf{x^n}) = p(x_1, x_2, ..., x_n) = \prod_{i=1}^{n} p(x_i)$. *Then there exists a constant* c *such that*

$$H(X) \leq \frac{1}{n} \sum_{\mathbf{x^n}} p(\mathbf{x^n}) K(\mathbf{x^n}|n) \leq H(X) + \frac{|Q| \log n}{n} + \frac{c}{n} \tag{4.1}$$

for all n. *Therefore,* $E\frac{1}{n}K(\mathbf{X^n}|n) \to H(X)$.

We recall here the monotone decreasing property of the entropy of configurations as stated in Theorem (3.1). From this theorem and the above theorem by Kolmogorov we have

Theorem 4.2 *Let* $K^t(\mathbf{X^n}|n)$ *be the conditional Kolmogorov complexity of the string* $\mathbf{x^n}$ *contained by* c^t. *The we have, for* $n \to \infty$,

$$E\frac{1}{n}K^t(\mathbf{X^n}|n) \geq E\frac{1}{n}K^{t+1}(\mathbf{X^n}|n) \tag{4.2}$$

The equality holds if and only if $I(\mathbf{X^n}; c^t|c^{t+1}) = 0$.

5 Concluding Remarks

A further research topics will be to find a new information measure for individual configurations and investigate its behavior during CA dynamics.

A conjecture: Let x be any consecutive finite portion of any configuration c and denote its Kolmogorov complexity by $K_c(x)$. Then $K_c(x) + constant \geq K_{F(c)}(x')$, where x' is the corresponding finite portion of x in $F(c)$: $x' = F(x)$.

References

[Cover&Thomas91] *Elements of Information Theory*, by Thomas M.Cover and Joy A.Thomas,1991,John Wiley & Sons, 542pp.

[Nishio&Saito02] H. Nishio and T. Saito, Information Dynamics of Cellular Automata II:Completeness, Degeneracy and Entropy, presented at 8th IFIP WG1.5 Conference, Prague, Chech Rep.. September 12. 2002.(manuscript available in 122KB pdf)

[Nishio&Saito03] H. Nishio and T. Saito, Information Dynamics of Cellular Automata I: An Algebraic Study, submitted for publication to *Fundamenta Infor-*